Version of 9.6.03

Rings and Fields

4. Unique Factorisation Domains

4A Associates Let R be an integral domain.

(a) If a, $b \in R$, then b is an **associate** of a if there is an invertible element e of R such that $b = ea$.

(b)(i) If $a \in R$ then $a = 1a$ so a is an associate of itself. **(ii)** If a is an associate of b, there is an invertible e such that $a = be$; now e^{-1} is invertible and $b = e^{-1}a$ so b is an associate of a. **(iii)** If a is an associate of b and b is an associate of c, there are invertible e, e' such that $a = eb$ and $b = e'c$; now ee' is invertible and $a = ee'c$ so a is an associate of c.

Thus 'is an associate of' is an equivalence relation.

(c)(i) The only associate of 0 is 0 itself.

(ii) The associates of 1 are the invertible elements of R.

(iii) If $p \in R$ is irreducible, then every associate of p is irreducible. **P** Suppose that q is an associate of p. Then q is non-zero and non-invertible because p is (using (i)-(ii) just above). If $q = ab$, let e be an invertible element of R such that $p = eq$; then $p = (ea)b$. Because p is irreducible, one of ea, b must be invertible. If ea is invertible, so is $a = e^{-1}(ea)$; so one of a, b must be invertible. As a, b are arbitrary, q is irreducible. **Q**

(iv) If $p \in R$ is prime, then every associate of p is prime. **P** Suppose that q is an associate of p. Then q is non-zero and non-invertible. Now suppose that $qr = ab$. Let $e \in R$ be an invertible element such that $q = pe$; then $per = ab$, so ab is a multiple of p and one of a, b is a multiple of p. If a is a multiple of $p = e^{-1}q$, then a is a multiple of q; if b is a multiple of p then b is a multiple of q. **Q**

(d)(i) If a, $b \in R$ then a and b are associates iff each is a multiple of other. (If $a = 0$ this is trivial. If $a \neq 0$ and $a = be$, $b = ae'$ then $a = aee'$ so $ee' = 1$ and e is invertible.) **(ii)** If a, $b \in R$ then a and b are associates iff they have the same multiples in R. **(iii)** If a, $b \in R$ then a and b are associates iff they have the same factors in R.

(e) Examples (i) In $\mathbb{Z}$, the associates of any $n \in \mathbb{Z}$ are $\pm n$. **(ii)** In $\mathbb{Q}[x]$, the associates of any polynomial are the non-zero constant multiples of that polynomial.

4B Definition A **unique factorisation domain** is an integral domain R such that for every non-zero, non-invertible $a \in R$

(i) there are irreducible elements $p_1, \dots, p_n \in R$ such that $a = p_1 \dots p_n$ (allowing $n = 1$ if a itself is irreducible);

(ii) if $q_1, \dots, q_m$ are further irreducible elements of R such that $a = q_1 \dots q_m$ then $m = n$ and the q_k can be re-ordered in such a way as to make each q_k an associate of p_k.

Example In $\mathbb{Z}$, we can express 60 as a product of irreducibles in various ways; for instance, $60 = 2.2.3.5 = 3.(-2).(-5).2$. But all such expressions have four factors and in all such expressions the factors are ± 2, ± 2, ± 3, ± 5 in some order.

4C Proposition Let R be an integral domain. Then the following are equivalent:

(i) R is a unique factorisation domain;

(ii) Irreducible elements of R are prime and every non-zero, non-invertible element of R is expressible as a product of irreducible elements.

proof (a)(i)⇒(ii) Suppose that R is a unique factorisation domain. Then of course every non-zero, non-invertible element is expressible as a product of irreducibles. To see that irreducibles are prime, let p be irreducible, and suppose that p is a factor of ab; that $pc = ab$. If either a or b is 0, then it is a multiple of p; if either a or b is invertible then the other is a multiple of p. If none of these happen, then $ab \neq 0$ (because R is an integral domain) so $c \neq 0$; also, because p is irreducible, it cannot be a multiple of ab, so c is not invertible.

We may therefore express a, b, c as products of irreducibles,

$$a = q_1 \dots q_k,\ b = q'_1 \dots q'_m,\ c = p_1 \dots p_n$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX and get $pp_1 \dots p_n = q_1 \dots q_k q'_1 \dots q'_m$. Because factorisation in R is unique, we must have $k + m = 1 + n$ and also p must be an associate of one of the q_i or q'_j. But in this case, because every q_i is a factor of a and every q'_j is a factor of b, p is a factor of at least one of a, b. As a and b are arbitrary, p is prime, as required.

(b)(ii)⇒(i) Now suppose that R satisfies the two conditions. To show that R is a unique factorisation domain we need to prove (ii) of 4C. Do this by induction on n. If $n = 1$ we have $p_1 = q_1 \dots q_m$; but as p_1 is irreducible all but one of the q_i must be invertible, and this means that $m = 1$ and $q_1 = p_1$ is an associate of p_1. For the inductive step to $n+1$ we have $p_1 \dots p_n p_{n+1} = q_1 \dots q_m$. Now this means that p_{n+1} is a factor of $q_1 \dots q_m$; but p_{n+1} is irreducible and we are supposing that irreducibles are prime, so p_{n+1} is a factor of q_k for some $k \le m$. Since q_k is also irreducible, there must be an invertible e such that $q_k = ep_{n+1}$. Now we have

$$p_1 \dots p_n = eq_1 \dots q_{k-1} q_{k+1} \dots q_m$$

(because R is an integral domain, so we may cancel p_{n+1} from both sides). But eq_1 (or eq_2, if $k = 1$) is also irreducible (4A(c-iii)), so the inductive hypothesis tells us that $n = m-1$ and that $eq_1, \dots , q_{k-1}, q_{k+1}, \dots , q_m$ can be got by shuffling $p_1, \dots , p_n$ and multiplying them by appropriate invertible elements. But this means that $n = m + 1$ and (since $q_k = ep_{n+1}$) the whole list $q_1, \dots , q_m$ can be got by shuffling $p_1, \dots , p_{n+1}$ and multiplying them by invertible elements. Thus the induction proceeds.

4D Theorem (a) Every principal ideal domain is a unique factorisation domain.
(b) Every Euclidean domain is a unique factorisation domain.

proof (a) Let R be a principal ideal domain. In 3we saw that irreducibles in R are prime; in 3we saw that every non-zero, non-invertible element of R is a product of irreducibles. And of course R is an integral domain. So 4C tells us that R is a unique factorisation domain.

(b) By 3every Euclidean domain is a principal ideal domain; by (a), it is also a unique factorisation domain.

4E Greatest common divisors Let R be a unique factorisation domain. If $a_1, \dots , a_n$ are non-zero elements of R, a **greatest common divisor** of $a_1, \dots , a_n$ is a $c \in R$ such that (i) c is a factor of every a_k (that is, every a_k is a multiple of c (ii) if d is any other common divisor of $a_1, \dots , a_n$ then c is a multiple of d.

4F Lemma Let R be a unique factorisation domain.
(a) If c is a greatest common divisor of $a_1, \dots , a_n \in R \setminus \{0\}$ and $b \in R \setminus \{0\}$, then bc is a greatest common divisor of $ba_1, \dots , ba_n$.
(b) If $a_1, \dots , a_n \in R \setminus \{0\}$, where $n \ge 1$, then they have a greatest common divisor.
(c) If c is a greatest common divisor of $a_1, \dots , a_n \in R \setminus \{0\}$, then there are $a'_1, \dots , a'_n$ such that $a_k = ca'_k$ for each $k \le n$, and now 1 is a greatest common divisor of $a'_1, \dots , a'_n$.

proof Define $\nu : R \setminus \{0\} \to \mathbb{N} \cup [\{0\}$ by writing $\nu(a) = 0$ if a is invertible, and $\nu(a) = m$ if $a = p_1 \dots p_m$ where $p_1, \dots , p_m$ are irreducible; because R is a unique factorisation domain, ν is well-defined.

(a) I show by induction on m that if $\nu(b) = m$ then bc is a greatest common divisor of $ba_1, \dots , ba_n$.
The induction starts with $m = 0$, in which case b is invertible, so that the factors of ba_k are precisely the factors of a_k, for each k, and the common divisors of $ba_1, \dots , ba_n$ are just the common divisors of $a_1, \dots , a_k$; accordingly c and bc are greatest common divisors of $ba_1, \dots , ba_n$.
Next, if $m = 1$, then b is irreducible, therefore prime. Of course bc is a factor of ba_k for every k. Now suppose that d is a common divisor of $ba_1, \dots , ba_n$. If d is a multiple of b, say $d = bd'$, then ba_k is a multiple of bd', so a_k is a multiple of d', for every k; accordingly d' is a common divisor of the a_k, and must be a factor of c, so that $d = bd'$ is a factor of bc. If d is invertible, then of course it is a factor of bc. If d is not a multiple of b, then for each k we can express ba_k as da'_k. Now da'_k is a multiple of b, but d is not, so a'_k is a multiple of b; say $a'_k = ba_k$", $ba_k = bda_k$". Cancelling b, we have $a_k = da_k$". But this is true for each k, so d is a common divisor of $a_1, \dots , a_k$ and is a factor of c, therefore of bc. Thus in any case d is a factor of bc and bc is a greatest common divisor of $a_1, \dots , a_n$.
Now, for the inductive step to $m > 1$, if $\nu(b) = m$ then we can express b as pb' where $\nu(b') = m - 1$. By the inductive hypothesis, $b'c$ is a greatest common divisor of $b'a_1, \dots , b'a_n$. By the case $m = 1$, $pb'c$ is

a greatest common divisor of $pb'a_1, \dots, pb'a_n$; that is, bc is a greatest common divisor of $ba_1, \dots, ba_n$, and the induction continues.

(b) Now I show by induction on $\nu(a_1)$ that if $a_1, \dots, a_n \in R \setminus \{0\}$ then $a_1, \dots, a_n$ have a greatest common divisor. The induction starts with the case $\nu(a_1) = 0$; in this case a_1 is invertible, so all its factors are invertible, and 1 is a greatest common divisor of $a_1, \dots, a_n$. For the inductive step to $\nu(a_1) = m > 0$, if 1 is a greatest common divisor of $a_1, \dots, a_n$ we can stop. Otherwise, they have a non-invertible greatest common divisor, which has an irreducible factor; so there is an irreducible $p \in R$ which is a common factor of $a_1, \dots, a_n$. Express a_k as pa'_k for each k. Then $\nu(a'_1) = m - 1$ so by the inductive hypothesis $a'_1, \dots, a'_n$ have a greatest common divisor c' say. Now by (a) of this proposition, pc' is a greatest common divisor of $a_1, \dots, a_n$. Thus the induction continues.

(c) Because c is a factor of a_k, we can find for each $k \le n$ an a'_k such that $a_k = ca'_k$. By (b), $a'_1, \dots, a'_k$ have a greatest common divisor c' say, and now cc' is a greatest common divisor of $a_1, \dots, a_k$, by (a); but this means that c is a multiple of cc', say $c = cc'd$, and $c'd = 1$, so that c' is invertible. Consequently all common divisors of $a'_1, \dots, a'_n$ are invertible and 1 is a greatest common divisor of $a'_1, \dots, a'_n$, as claimed.

4G Primitive polynomials Let R be a unique factorisation domain. A non-zero polynomial $f \in R[x]$ is **primitive** if 1 is a greatest common divisor of its non-zero coefficients.

If $f \in R[x]$ is any non-zero polynomial, let c be a greatest common divisor of its non-zero coefficients; then f can be expressed as cg where g is primitive (using 4Fc).

4H Proposition Let R be a unique factorisation domain. If f and g are primitive polynomials in $R[x]$, then $f \times g$ is still primitive.

proof ? Suppose, if possible, otherwise; that the non-zero coefficients of $f \times g$ have a non-invertible common divisor. Then they have an irreducible common divisor p say, which is prime. Suppose $f = \sum_{i=0}^{m} a_i x^i$, $g = \sum_{i=0}^{n} b_i x^i$. There must be $j \le m$, $k \le n$ such that p is not a factor of a_j nor of b_k; take the least such. Now examine the coefficient c of x^{j+k} in $f \times g$. This is supposed to be a multiple of p. But also we have

$$c = a_0 b_{j+k} + a_1 b_{j+k-1} + \ldots + a_j b_k + \ldots + a_{j+k} b_0.$$

So

$$a_j b_k = c - a_0 b_{j+k} - \ldots - a_{j-1} b_{k+1} - a_{j+1} b_{k-1} - \ldots - a_{j+k} b_0.$$

All the terms on the right are multiples of p (because a_i is a multiple of p if $i < j$, while b_i is a multiple of p if $i < k$), so $a_j b_k$ is a multiple of p. Because p is prime, either a_j or b_k must be a multiple of p; which is absurd. **X**

4I Lemma Let R be a unique factorisation domain and F its field of fractions. If f is any non-zero polynomial in $F[x]$, then it is expressible as γg where $\gamma \in F$ and $g \in R[x]$ is primitive in $R[x]$.

proof We can express f as $\sum_{j=0}^{n} \frac{a_j}{b_j} x^j$, where each $a_j \in R$ and each $b_j \in R \setminus \{0\}$, and not every a_j is zero. Set $b = b_0 \dots b_n$, so that $b \ne 0$; set $a'_j = b\frac{a_j}{b_j} \in R$ for each j. Let c be a greatest common divisor of the non-zero a'_j; then we can express these in the form $ca"_j$, where the $a"_j$ have 1 as a greatest common divisor. Setting $a"_j = 0$ if $a'_j = 0$, we see that $g = \sum_{j=0}^{n} a"_j x^j$ is primitive and $f = \frac{c}{b} g$.

4J Proposition Let R be a unique factorisation domain and F its field of fractions. Suppose that $f \in R[x]$ is primitive in $R[x]$. If $g \in F[x]$ is such that $f \times g \in R[x]$ then $g \in R[x]$.

proof If $g = 0$ this is trivial. Otherwise, we may express g as γg_1, where $\gamma \in F$ and $g_1 \in R[x]$ is primitive, by 4I; express γ as $\frac{c}{d}$ where c, $d \in R \setminus \{0\}$. Set $h = f \times g_1$; then h is primitive in $R[x]$, by 4H, and $\gamma h = f \times g \in R[x]$. This means that if $h = \sum_{j=0}^{n} b_j x^j$, $\gamma b_j \in R$ for every j, that is, d is a factor of $cb_j = d\gamma b_j$ for every j. But by 4Fa, c is a greatest common divisor of the non-zero cb_j, so c is a multiple of d in R and $\gamma = \frac{c}{d} \in R$. Accordingly $g = \gamma g_1 \in R[x]$.

4K A note on constant polynomials For any ring R, $c \in R$ we have the corresponding constant polynomial $\tilde{c} = c + 0x + 0x^2 + \ldots \in R[x]$. Observe that $\tilde{c} + \tilde{d} = (c+d)\tilde{}$, $\tilde{c} \times \tilde{d} = (cd)\tilde{}$; that is, $c \mapsto \tilde{c}$ is a ring homomorphism from R to $R[x]$; and of course this homomorphism is injective. If R has a **1**, then $\tilde{1}$ is a **1** in $R[x]$. If $c \in R$ is invertible in R, then $\tilde{c}$ is invertible in $R[x]$ (because if $cd = dc = 1$ in R, then $\tilde{c}\tilde{d} = \tilde{d}\tilde{c} = \tilde{1}$). Conversely, if $c \in R$ and $\tilde{c}$ is invertible in $R[x]$, then c must be invertible in R (because if $\tilde{c} \times f = f \times \tilde{c} = \tilde{1}$ in $R[x]$, then $cd_0 = d_0 c = 1$ in R, where $f = d_0 + d_1 x + \ldots$.

If R is an integral domain, then a product $f \times g$ in $R[x]$ can be constant only when one of f, g is zero or both are constant polynomials. Consequently $\tilde{c}$ will be irreducible in $R[x]$ iff c is irreducible in R.

4L Proposition Let R be a unique factorisation domain and F its field of fractions. If $f \in R[x]$ then the following are equivalent:
(i) f is non-constant and irreducible in $R[x]$;
(ii) f is primitive in $R[x]$ and irreducible in $F[x]$.

proof (a)(i)⇒(ii) Suppose that f is non-constant and irreducible in $R[x]$.

(α) **?** If f is not primitive, let c be a greatest common divisor of its non-zero coefficients; then c is non-invertible in R. We have $f = cg$ for some $g \in R[x]$, where by $c\sum_{j=0}^{n} a_j x^j$ I mean $\sum_{j=0}^{n} ca_j x^j$; but now $f = \tilde{c} \times g$, where $\tilde{c}$ is the constant polynomial corresponding to c, and $\tilde{c} \times g$ is the product in the ring $R[x]$. Because c is non-invertible in R, $\tilde{c}$ is non-invertible in $R[x]$; because f is non-constant, g is non-constant, so non-invertible in $R[x]$ (because R is an integral domain). Thus f is not irreducible, contrary to hypothesis. **X**

So f is primitive.

(β) **?** Suppose, if possible, that f is not irreducible in $F[x]$. Then we can express f as $g \times h$ where neither g nor h is invertible in $F[x]$. Of course neither can be zero, and indeed neither can be constant, because F is a field, so every non-zero constant polynomial is of the form $\tilde{\gamma}$ where γ is invertible in F, and is therefore invertible in $F[x]$. Now we can express g as γg_1 where $\gamma \in F$ and $g_1 \in R[x]$ is primitive in $R[x]$ (4I), and now $g_1 \times (\gamma h) = f \in R[x]$. By 4J, $h_1 = \gamma h \in R[x]$, and $f = g_1 \times h_1$ is a factorisation of f in $R[x]$. Because neither g_1 nor h_1 is invertible, f is not irreducible in $R[x]$, contrary to hypothesis. **X**

(b)(ii)⇒(i) Now suppose that f is primitive in $R[x]$ and irreducible in $F[x]$. Then it cannot be constant, because constant polynomials are either zero or invertible in $F[x]$. Suppose that $f = g \times h$ in $R[x]$. Then $f = g \times h$ in $F[x]$ also, so one of g, h must be invertible in $F[x]$, and therefore constant; suppose that $g = \tilde{c}$ is constant. Then c is a common divisor of the coefficients of $f = ch$; but f is primitive, so c is invertible in R, and $g = \tilde{c}$ is invertible in $R[x]$. As g, h are arbitrary, f is irreducible in $R[x]$.

4M Proposition Let R be a unique factorisation domain. Then irreducibles in $R[x]$ are prime in $R[x]$.

proof Let $f \in R[x]$ be irreducible, and suppose that $g, h \in R[x]$ are such that f is a factor of $g \times h$. I need to prove that one of them is a multiple of f. If either g or h is 0, then of course it is a multiple of f; so let us suppose that g, h are both non-zero.

case 1 Suppose that f is constant; then it is of the form $\tilde{p}$ where $p \in R$ is irreducible in R (see 4K). Express g as cg_1 and h as dh_1, where $c, d \in R$ and $g_1, h_1 \in R[x]$ are primitive (4G). Then $f = \tilde{p}$ is a factor of $g \times h = cd(g_1 \times h_1)$, and p is a common divisor of the coefficients of h. But as $g_1 \times h_1$ is primitive (4H), cd is a greatest common divisor of the non-zero coefficients of h, so p is a factor of cd.

Now p is irreducible in R and R is a unique factorisation domain, so p is prime in R. Accordingly one of c, d is a multiple of p. If c is a multiple of p, then $g = cg_1$ is a multiple of $\tilde{p} = f$; if d is a multiple of p then h is a multiple of f.

case 2 Suppose f is not constant. By 4L, f is primitive in $R[x]$ and irreducible in $F[x]$. But $F[x]$ is a Euclidean domain (), so irreducibles in $F[x]$ are prime in $F[x]$ (); while of course f is still a factor of $g \times h$ in $F[x]$. So f is a factor of one of g, h in $F[x]$. Suppose the former; then there is a $g_1 \in F[x]$ such that $f \times g_1 = g$. But as f is primitive in $R[x]$, it follows that $g_1 \in R[x]$, by 4J. So f is a factor of g in $R[x]$. Similarly, if f is a factor of h in $F[x]$ then it is still a factor of h in $R[x]$; and one of these has to happen.

Thus in either case f is a factor of one of g, h in $R[x]$; as g and h are arbitrary, f is prime in $R[x]$.

4N Proposition Let R be a unique factorisation domain. If $f \in R[x]$ is non-zero and non-invertible, then it is expressible as a product of irreducibles in $R[x]$.

proof: case 1 Suppose that $f = \tilde{c}$ is a constant polynomial. Then c is non-zero and non-invertible in R (4K), so is expressible as a product $p_1 \ldots p_n$ where $p_1, \ldots, p_n$ are irreducible in R. Now $f = \tilde{c} = \tilde{p}_1 \ldots \tilde{p}_n$ in $R[x]$, and each $\tilde{p}_k$ is irreducible in $R[x]$ (see 4K again), so f is a product of irreducibles in $R[x]$.

case 2 Suppose f is non-constant and primitive in $R[x]$. Because $F[x]$ is a Euclidean domain, f is expressible as a product $g_1 \times \ldots \times g_n$ of irreducibles in $F[x]$ (). Note that no g_k can be constant because all non-zero constant polynomials in $F[x]$ are invertible in $F[x]$. Express each g_k as $\gamma_k g'_k$ where $\gamma_k \in F$ and $g'_k \in R[x]$ is primitive in $R[x]$ (4I). Because $g'_k = \tilde{\gamma}_k \times g_k$ is an associate of g_k in $F[x]$, it is irreducible in $F[x]$ (4A(c-iii)); being primitive in $R[x]$, it is also irreducible in $R[x]$ (4L). Then $f = \gamma g = \tilde{\gamma} g$, where $\gamma = \gamma_1 \ldots \gamma_n \in F$ and $g = g_1 \times \ldots g_n \in R[x]$; note that g is primitive (4H). Consequently $\tilde{\gamma} \in R[x]$ (4J) and $\gamma \in R$. Now γ is a common divisor of the coefficients of f, and f is primitive in $R[x]$, so γ must be invertible in R. Thus $\gamma g'_1 = \tilde{\gamma} \times g'_1$ is an associate of g'_1 in $R[x]$ and is irreducible in $R[x]$. Finally $f = (\gamma g'_1) \times \ldots \times g'_n$ is a product of irreducibles in $R[x]$.

case 3 Suppose that f is neither constant nor primitive. Then f is expressible as $cg = \tilde{c} \times g$ where $c \in R$ and g is primitive (4G); because f is not itself primitive, c is not invertible; because f is not constant, nor is g, so g also is not invertible. By case 1, $\tilde{c}$ is a product of irreducibles in $R[x]$; by case 2, g is a product of irreducibles in $R[x]$; putting these together, f is a product of irreducibles in $R[x]$.

4O Theorem If R is a unique factorisation domain, so is $R[x]$.

proof Put 4M, 4N and 4C together.

4P Corollary (a) $\mathbb{Z}[x]$ is a unique factorisation domain.
(b) For any field F, $F[x, y]$ is a unique factorisation domain.
(c) $\mathbb{Z}[x, y, z]$ is a unique factorisation domain.

4Q Remarks (a) The point of the work above is that the rings in 4P are not principal ideal domains, therefore cannot be dealt with by the theorems of §3. (To see that $\mathbb{Z}[x]$ is not a principal ideal domain, consider the ideal of polynomials with *even* constant coefficient; this is not a principal ideal. To see that $F[x, y]$ is never a principal ideal domain, consider the ideal of polynomials of the form $f \times x + g \times y$; this is not a principal ideal.) These rings are of such importance that it is worth going to a great deal of trouble over them.

(b) A notable feature of the proofs here is that they make essential use of the field of fractions F of the given unique factorisation domain R. The ring $F[x]$, being a Euclidean domain, is essentially easier to deal with; the bulk of the argument is a careful translation of facts about $F[x]$ into facts about $R[x]$.

(c) The arguments above are cast in a very abstract form. Most students will find it useful to read them through at least once imagining that $R = \mathbb{Z}$ and $F = \mathbb{Q}$ throughout; the essential ideas remain unaffected, but for 'invertible element of R' you will be able to read '± 1', and for 'irreducible element of R' you will be able to read '$\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \ldots$'.

I have tried to be careful, wherever both R and its field of fractions F are both present, to say explicitly whether ring elements or polynomials are invertible, or irreducible, or prime in R, or F, or $R[x]$, or $F[x]$ as appropriate. The point is that, for instance, 2 is irreducible in $\mathbb{Z}$ but invertible in $\mathbb{Q}$; while $2 + 2x$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$ (its factorisation as $\tilde{2} \times (1 + x)$ is non-trivial in $\mathbb{Z}[x]$, but trivial in $\mathbb{Q}[x]$, because $\tilde{2}$ is invertible in $\mathbb{Q}[x]$).

The abstract form is necessary, of course, if we wish to extend these ideas to show that $\mathbb{Z}[x, y]$ (for instance) is a unique factorisation domain.

6. Fermat's Last Theorem

This celebrated conjecture states: If x, y, z and n are strictly positive integers, and $n \geq 3$, then $x^n + y^n \neq z^n$. It was finally proved by Andrew Wiles in 1993-1995.

Proofs of special cases have created large parts of the modern theory of rings and fields. There is an essentially elementary proof of the case $n = 4$ (see 6G-6J below). In 6A-6F here I set out a proof for the case $n = 3$, taken from HARDY & WRIGHT 65, §13.4.

6A Set $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \exp(\frac{2\pi i}{3}$, so that $\omega^3 = 1$ and $1 + \omega + \omega^2 = 1$. We shall need the fact that $x^3 + y^3 = (x + y)(x + \omega y)(x + \omega^2 y)$, $x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$ for all x, $y \in \mathbb{C}$.

Let R be the ring $\{m + n\omega : m, n \in \mathbb{Z}\}$; then R is a Euclidean domain if given the valuation $\nu(a) = |a|^2$ for $a \in R \setminus \{0\}$. The invertible elements of R are just those with $\nu(a) = 1$, that is, taking them in order around the unit circle, 1, $-\omega^2$, ω, -1, ω^2, $-\omega$.

For the rest of this chapter, write $\lambda = 1 + 2\omega = i\sqrt{3} \in R$. Then $\nu(\lambda) = 3$ is a prime in $\mathbb{Z}$ so λ is irreducible in R.

The arguments below will rely repeatedly on the fact that R, being a Euclidean domain, is a unique factorisation domain.

6B Lemma If $a \in R$ then $a \equiv 0$, 1 or -1 modulo λ.

proof Because R is a Euclidean domain, we know that a is expressible as $q\lambda + r$ where either $r = 0$ or $\nu(r) < \nu(\lambda) = 3$. Now if $a = m + n\omega \in R$ then $|a|^2 = m^2 - mn + n^2 = (m - \frac{1}{2}n)^2 + \frac{3}{4}n^2 \neq 2$, so the only members of R of modulus less than $\sqrt{3}$ are

0,
1, $\omega = 1 - \omega^2\lambda \equiv 1$, $\omega^2 = 1 + \omega\lambda \equiv 1$,
-1, $-\omega \equiv -1$, $-\omega^2 \equiv -1$.

So r must be congruent to one of 0, 1 and -1 modulo λ, and a is the same.

6C Lemma If $a \in R$ and $a \equiv \epsilon$ modulo λ, where $\epsilon = \pm 1$, then $a^3 \equiv \pm\epsilon$ modulo 9.

proof: case 1 If $a \equiv 1$ modulo λ, then $a = b\lambda + 1$ for some $b \in R$. Now, as remarked above, $1 - \omega$ and $1 - \omega^2$ are both multiples of λ; more specifically, $1 - \omega = \lambda(1 + \omega\lambda)$ and $1 - \omega^2 = \lambda(-1 + \omega^2\lambda)$. So

$$\begin{aligned} a^3 - 1 &= (a-1)(a-\omega)(a-\omega^2) \\ &= b\lambda(b\lambda + \lambda(1+\omega\lambda))(b\lambda + \lambda(-1+\omega^2\lambda)) \\ &= \lambda^3 b(b+1+\omega\lambda)(b-1+\omega^2\lambda) \\ &= \lambda^3 b(b-1)(b+1) + \lambda^4 c \end{aligned}$$

for some $c \in R$. But $b(b-1)(b+1)$ is divisible by λ, by 6B; so $a^3 - 1$ is divisible by $\lambda^4 = 9$, as claimed.

case 2 If $a \equiv -1$ modulo λ then $-a \equiv 1$ modulo 9; by case 1, $(-a)^3 \equiv 1$ and $a^3 \equiv -1$ modulo 9.

6D Lemma If $n \geq 1$ is an integer, a, b, c are members of R not divisible by λ, e, e' and e'' are invertible in R, and

$$e\lambda^{3n}a^3 + e'b^3 + e''c^3 = 0,$$

then (a) $n \geq 2$ (b) there are an invertible $e_1 \in R$ and $c_1 = \pm c \in R$ such that

$$e_1\lambda^{3n}a^3 + b^3 + c_1^3 = 0.$$

proof Take ϵ, ϵ', $\epsilon'' \in \{1, -1\}$ such that $a \equiv \epsilon$, $b \equiv \epsilon'$, $c \equiv \epsilon''$ modulo λ (using 6B). Then we have $e\lambda^{3n}\epsilon + e'\epsilon' + e''\epsilon'' \equiv 0$ modulo 9, by 6C. So $e'\epsilon' + e''\epsilon''$ must be divisible by λ^3. But on the other hand $|e'\epsilon' + e''\epsilon''| \leq 2 < |\lambda|^3$, so $e'\epsilon' + e''\epsilon'' = 0$. Consequently $e\lambda^{3n}\epsilon$ is divisible by $9 = \lambda^4$. But this means that $3n \geq 4$ and $n \geq 2$.

Next, because $e'\epsilon' + e''\epsilon'' = 0$, $e'' = \pm e'$. Setting $e_1 = (e')^{-1}e$ and $c_1 = (e')^{-1}e''c$, we have $c_1^3 = (e')^{-1}e''c^3$ so

$$e_1\lambda^{3n}a^3 + b^3 + c_1^3 = (e')^{-1}(e\lambda^{3n}a^3 + e'b^3 + e''c^3) = 0,$$

as required.

6E Lemma If $n \geq 1$ is an integer and a, b, c are coprime members of R not divisible by λ, and if $e \in R$ is invertible, then $e\lambda^{3n}a^3 + b^3 + c^3 \neq 0$.

Notation In any unique factorisation domain, we say that $a_1, \ldots, a_n$ are **coprime** if they have no non-invertible common divisor, that is, if 1 is a greatest common divisor of $a_1, \ldots, a_n$.

proof Induce on n. For $n = 1$ this is covered by 6D.

For the inductive step to $n+1$, **?** suppose, if possible, that $e\lambda^{3n+3}a^3 + b^3 + c^3 = 0$. Then

$$-e\lambda^{3n+3}a^3 = (b+c)(b+\omega c)(b+\omega^2 c).$$

Consider the expansion of the right-hand-side into irreducible factors. We note first that

$$\begin{gathered} (b+c) - (b+\omega c) = (1-\omega)c = \omega^2\lambda c, \\ (b+\omega c) - (b+\omega^2 c) = \lambda c, \\ (b+\omega^2 c) - (b+c) = \omega\lambda c \end{gathered}$$

are all divisible by λ, but none are divisible by λ^2, because c is not divisible by λ and ω, ω^2 are invertible. Accordingly (since R is a unique factorisation domain and λ is a prime in R which surely divides $-e\lambda^{3n+3}a^3$), all the factors $b+c$, $b+\omega c$, $b+\omega^2 c$ are divisible by λ, and exactly one of them is divisible by λ^{3n+1}.

We see also that no two of

$$b+c,\ b+\omega c,\ b+\omega^2 c$$

can have a non-trivial irreducible common factor other than λ, since if they did it would be a factor of c and therefore of b as well, and also of a; and we are supposing that a, b, c are coprime. The irreducible factors of a^3 come in threes, which must therefore be distributed among the factors of $b+c$, $b+\omega c$, $b+\omega^2 c$ as cubes (but possibly with invertible elements attached). (This is the point at which we most essentially use the fact that R is a unique factorisation domain.) Thus we must have

$$b+c,\ b+\omega c,\ b+\omega^2 c$$

equal to

$$e_1\lambda^{3n+1}d_1^3,\ e_2\lambda d_2^3,\ e_3\lambda d_3^3$$

in some order, where d_1, d_2, $d_3 \in R$ are coprime and not divisble by λ, and e_1, e_2, e_3 are invertible. Taking c_1 to be either c or ωc or $\omega^2 c$, we get

$$b+c_1 = e_1\lambda^{3n+1}d_1^3;$$

now (switching the subscripts $_2$, $_3$ if need be) we have

$$b+\omega c_1 = e_2\lambda d_2^3,\ b+\omega^2 c_1 = e_3\lambda d_3^3.$$

Now consider

$$\begin{aligned} 0 &= (1+\omega+\omega^2)(b+c_1) \\ &= (b+c_1)+\omega(b+\omega c_1)+\omega^2(b+\omega^2 c_1) \\ &= e_1\lambda^{3n+1}d_1^3 + e_2\omega\lambda d_2^3 + e_3\omega^2\lambda d_3^3. \end{aligned}$$

Cancelling λ, we have

$$0 = e_1\lambda^{3n}d_1^3 + e_2\omega d_2^3 + e_3\omega^2 d_3^3.$$

But now by 6D there are $\tilde{e}_1$, $\tilde{d}_3$ such that $\tilde{e}_1$ is invertible, $\tilde{d}_3 = \pm d_3$ and

$$0 = \tilde{e}_1\lambda^{3n}d_1^3 + d_2^3 + \tilde{d}_3^3,$$

which is impossible, by the inductive hypothesis. **X**

Thus the induction continues.

6F Theorem If a, b, $c \in R \setminus \{0\}$ then $a^3+b^3 \neq c^3$.

proof ? Suppose, if possible, otherwise. Let d be a greatest common divisor of a, b, c, and express a as da_1, b as db_1, c as $-dc_1$; then a_1, b_1, c_1 are coprime and $a_1^3+b_1^3+c_1^3=0$. (Here again we are using the fact that R is a unique factorisation domain.) Observe that any common prime factor of two of a_1, b_1, c_1 would have to be a factor of the cube of the third, and therefore a factor of all three; so no such prime factor exists, and no two of a_1, b_1, c_1 have a non-trivial common factor.

Calculating modulo 9, we see that we cannot have $\pm1\pm1\pm1 \equiv 0$ modulo 9, so that at least one of a_1, b_1, c_1 is divisible by λ, by 6C. Let us suppose that a_1 is divisible by λ and the others not. Then we can express a_1 as $\lambda^n a_2$ where λ is not a factor of a_2, and get

$$\lambda^{3n}a_2^3 + b_1^3 + c_1^3 = 0.$$

But by 6E this is impossible. The same obstacle arises if either b_1 or c_1 is divisible by λ. **X**

6F Corollary If a, b, $c \in \mathbb{N}$ then $a^3+b^3 \neq c^3$.

6G The case $n=4$ I add a note on the case $n=4$, which is essentially easier. It depends on the following remark on Pythagorean triples (i.e., triples $(a,b,c) \in \mathbb{N}^3$ such that $a^2+b^2=c^2$).

6H Proposition Let a, b, $c \in \mathbb{N}$ be such that $a^2+b^2=c^2$ and a, b are coprime. Then there are p, $q \in \mathbb{N}$ such that $\{a,b\} = \{2pq, p^2-q^2\}$, and in this case p, q are coprime; also $c = p^2+q^2$.

proof First note that c^2 must be congruent to either 0 or 1 modulo 4; because if c is even then c^2 is divisible by 4, while if c is odd then $c=(2d+1)^2 = 4(d^2+d)+1$ for some d. The same applies to a^2 and b^2. So, computing modulo 4, the equation $a^2+b^2=c^2$ becomes either $0+0=0$ or $0+1=1$ or $1+0=1$. The first is impossible because we are supposing that a, b are coprime. So we conclude that c must be odd and one of a, b is even, the other odd.

Suppose that a is even; say $a=2a_1$. Then $4a_1^2 = (c+b)(c-b)$. Now $c+b$, $c-b$ are either both even or both odd; they cannot both be odd, so both are even; say $c+b=2p_1$ and $c-b=2q_1$. We have $c=p_1+q_1$, $b=p_1-q_1$, $a^2=4p_1q_1$. So p_1 and q_1 are coprime. But $p_1q_1=a_1^2$ is a perfect square, so p_1 and q_1 must be perfect squares; say $p_1 = p^2$, $q_1 = q^2$. Now $a = 2pq$ and $b = p^2 - q^2$. Similarly, if a is odd and b is even, we can express a as $p^2 - q^2$ and b as $2pq$.

Of course p and q have to be coprime because p_1 and q_1 are. Because $c^2 = a^2 + b^2 = 4p^2q^2 + (p^2 - q^2)^2 = (p^2 + q^2)^2$, $c = p^2 + q^2$.

6I Proposition If a, b, $c \in \mathbb{N}$ then $a^4 + b^4 \neq c^2$.

proof Induce on c. For $c = 1$, this is trivial. For the inductive step to $c > 1$, **?** suppose, if possible, otherwise. Let d be the greatest common divisor of a, b in $\mathbb{N}$. Then d^4 is a factor of c^2 so d^2 is a factor of c. Express a as da_1, b as db_1, c as d^2c_1; then $a_1^4 + b_1^4 = c_1^2$, and a_1, b_1 are coprime. By the inductive hypothesis, $c_1 \geq c$, so in fact $c_1 = c$ and $d = 1$ and a, b are coprime.

By 6H, there are p, $q \in \mathbb{Z}$ such that one of a^2, b^2 is $2pq$ and the other is $p^2 - q^2$; thus $2pq$ and $p^2 - q^2$ are both perfect squares, while p and q are still coprime. Note that $p^2 - q^2$ must be odd, and that $c = p^2 + q^2$. Without loss of generality, we may take it that $b^2 = p^2 - q^2$, so that $b^2 + q^2 = p^2$. Once again, because $a^2 = 2pq$, b and q are coprime, so there are coprime p_1, q_1 such that $q = 2p_1q_1$ and $b = p_1^2 - q_1^2$ (note that b must be odd).

Now $a^2 = 2pq = 4pp_1q_1$ so pp_1q_1 is a perfect square; because p and $p_1q_1 = \frac{1}{2}q$ are coprime, p and p_1q_1 are perfect squares. Because p_1 and q_1 are coprime, they also are perfect squares. But now, if $p = \tilde{c}^2$, $p_1 = \tilde{a}^2$, $q_1 = \tilde{b}^2$ we have $\tilde{a}^4 + \tilde{b}^4 = \tilde{c}^2$, while $\tilde{a}$, $\tilde{b}$ are both non-zero.

By the inductive hypothesis, $\tilde{c} \geq c$. But this is absurd, because $c = p^2 + q^2$, so $\tilde{c}^2 = p < c$. **X**

Thus the induction continues.

6J Corollary If a, b, $c \in \mathbb{N}$ then $a^4 + b^4 \neq c^4$.

References

Hardy G.H. & Wright E.M. [65] *An Introduction to the Theory of Numbers.* Oxford U.P., 1965.